「サイバーセキュリティ戦略（案）」批判

2025年12月19日19時開始
マイクとカメラを切ってお待ちください

JCA-NETセミナー
2025/12/19

としまる
toshi@jca.apc.org



https://togetherforpalestine.bandcamp.com/album/lullaby

「サイバーセキュリティ戦略（案）」批判

JCA-NETセミナー
2025/12/19

としまる
toshi@jca.apc.org

本日のテーマ

政府は11月に新たな「サイバーセキュリティ戦略(案)」について、パブリックコメントを募集しました。今回の戦略案では、2021年に策定された現行のサイバーセキュリティ戦略と比較しても、政府によるサイバー領域への介入・統制の傾向が格段に前面に押し出されています。この戦略案では「アクセス・無害化措置を始めとする多様な手段を組み合わせた能動的な防御・抑止」という表現で日本によるサイバー攻撃の体制を官民一体となって準備する内容になっています。

今回の戦略案は、「サイバー戦争」の体制づくりを鮮明にして、国家安全保障を口実として、民間企業をも巻き込んで、私たちのネットにおけるコミュニケーションの根幹をなす通信の秘密や言論・表現に関わる通信情報の取得の体制構築に重点が置かれるなど、看過できないものになっています。今回のセミナーではこの戦略案について、JCA-NETが提出した意見の内容を紹介しながら、問題点について議論します。

サイバーセキュリティ戦略(案)の読み方

政府文書の基本的な記述の「戦略」

- **理念や建前**を述べる。たいていは、誰もが否定しがたい普遍的な理念などが抽象的に論じられる。この箇所は、**実際には何の政策上の約束や義務などとは関係がない。**(真に受けてはいけない部分)
- 政策を策定・実行する前提になる**事例や現状認識⇒この認識から、必要な対策**を導く。
  - 政府の国際政治についての考え方と戦略が前提にある。
  - 政府の戦略にとって好都合な現状の事例を例示。(**不都合な事実に言及しない**)
  - 提示した事例が客観的な現実であるかのような装いをとる。(**データの恣意的な引用**)
  - 実際の文書では、現状認識⇒政策の提案という順番になるので、あたかも政策(戦略)が現状の客観的な認識に基づいているかのような印象を与える。
  - 現状認識や例示に関連して、**人々の不安感情を喚起するような情緒的な表現**を折り込む。

サイバーセキュリティ戦略（案）の読み方

政府文書の基本的な記述の「戦略」

- 日本政府の国際政治理解は、友・敵関係を基礎にしており、国際関係の緊張を高める傾向にある。
- **「敵」の攻撃についての記述は、日本が攻撃を実行するときも、同じような（あるいはそれ以上の）行動をとるに違いないと考えておく必要がある。**
- サイバー領域は私たちのコミュニケーション（言論・表現の自由、思想信条の自由）の基盤⇒政府のサイバー戦争に巻き込まれることになる。⇒**サイバー戦争を推進する政府にわたしたちのコミュニケーションの権利を委ねることはできない。**

サイバーセキュリティ戦略(案)の構成

「脅威の増大」の原因への言及が皆無

目次

抑止=攻撃

https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000302319

サイバーセキュリティ戦略（案）の構成

新たな「サイバーセキュリティ戦略」（案）の全体像

○ **「国家安全保障戦略」**及び**サイバー対処能力強化法等**に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、**今後５年の期間を念頭に、**取るべき諸施策の目標や実施方針を内外に示す。

基本的な考え方

○ サイバー空間は、経済社会の持続的な発展、自由主義、民主主義、文化発展を支える基盤。

○ 法の支配、基本的人権の尊重といった普遍的価値に基づく国際秩序が深刻な危機にさらされ、サイバー脅威による国民生活・経済活動、ひいては国家安全保障上の懸念が高まっている。

「５つの原則」※を、引き続き「基本原則」として堅持した上で、国がこれまで以上に積極的な役割を果たすことで、厳しさを増すサイバー空間情勢に対応すべく施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することを明確化

（※施策の立案・実施原則となる「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」）

情勢認識

- 厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大
- 社会全体のデジタル化の進展とサイバー脅威の増大
- AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

施策の方向性

1 深刻化するサイバー脅威に対する防御・抑止

- 厳しいサイバー安全保障環境に対応するため、官民連携・国際連携の下、事案対処等の従来からの施策に能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、脅威を防御・抑止
- 政府から民間への積極的な情報提供

国が要となる防御・抑止

官民連携エコシステムの形成

国際連携の推進・強化

2 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

- 様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施（政府機関等が範となり対策）
- デジタル化とセキュリティ確保の同時推進

政府機関等の対策強化

重要ｲﾝﾌﾗ事業者・地方公共団体等の対策強化

サプライチェーン全体のﾚｼﾞﾘｴﾝｽ確保（中小企業・ベンダー等）

全員参加によるサイバーセキュリティ向上

ｻｲﾊﾞｰ犯罪対策を通じた安全・安心の確保

3 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

・産学官を通じたサイバー人材の確保・育成
・国産を核とした、新技術・サービスの創出

効率的・効果的な人材の育成・確保

新たな技術・サービスのエコシステム形成

先端技術(AI、量子技術等)への対応・取組

官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進
これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靱さを持つ国家を目指す。

批判：外交の位置付けがない

国家あるいは国家を後ろ盾とするサイバー攻撃には、政治的な動機がある。まず政府がすべき課題は、攻撃の動機そのものをなくす努力であり、これは外交が担うものである。日本の国際関係、とりわけ政府の対外政策の失敗が地域の緊張をもたらし、これがサイバー領域における攻撃の動機を生み出している。

日本の外交の役割は、こうした国際関係における緊張や対立を交渉や対話によって解決することにあり、こうした外交的努力は政府でしかなしえない役割である。

しかし、本案には、こうした外交的な取り組みの位置付けはほどんどないに等しく、外交への言及はたった１箇所だけであって、**サイバー領域における武力、戦力に該当するようなものも含めた力の行使への依存が著しい。**本案の考え方は、サイバー領域の安全保障にとっては逆効果にしかならない。少なくとも外交やサイバー領域における外務省や国連のいうヒューマンセキュリティ（私たちはこれをピープルズ・セキュリティと呼ぶ）といった観点からの戦略との関係が明確にされるべきであり、また、国家あるいは国家を後ろ盾とするサイバー攻撃の脅威アクターによる**攻撃の動機そのものをなくす**ためにどのような力によらない外交戦略をとるのか、といった観点が必須であるが、これが全く欠落している。このように、日本政府が取り組むべき基本的な課題は、サイバー領域におけるいわゆる地政学的な脅威とされる事態を取り除く外交努力であり、この位置付けが明確にされるべきである。

※日本が攻撃の動機をもたないようにするにはどうすべきか？

批判：政府の責務としての「動機の排除」

本案でも繰り返し言及されている**自由、公正かつ安全なサイバー空間**は、東アジアにおいて政府間で相互に敵対しあう関係とは相対的に切り離された領域として、**国益に左右されずに維持されること**が必要である。この点で、政府がサイバー空間においてなすべき第一の責務は、**サイバー領域において、人々が国境を越えた自由なコミュニケーションを実践できるような基盤を構築**することや民主主義の基盤をなす**検閲されずに自由に自らの思想・信条を伝えることを保障**すること、**通信の秘密をグローバルに保障**することである。少なくとも、いわゆる地政学的なリスクを軽減するためには、**軍事に依存しない外交や国際関係を構築**し、国家や国家を後ろ盾とするサイバー攻撃のアクターによる攻撃の動機を失なわせることであり、これこそが政府がまず第一に取り組むべきサイバーセキュリティの戦略的な課題である。本案は、**攻撃のリスクを軽減する最も本質的で基本的な国家の責任を回避**するものであって、到底受け入れがたい。

「戦略（案）」に記載されている攻撃の事例

国家によるサイバー攻撃の事例

- ロシア：軍事的・政治的目的の達成
- 中国：企業の情報窃取、重要インフラの機能妨害・破壊
- 朝鮮：資金調達

刻・致命的な被害を生じさせるおそれが現実のものとなっている。

我が国を取り巻く安全保障環境において特に注目すべき国・地域も、サイバー攻撃の国家的な利用を行っているとみられている。ロシアはサイバー攻撃を軍事的・政治的目的達成のために利用しているとみられ、2022 年のウクライナ侵略前に、同国の政府機関や重要インフラ事業者等の情報システム・ネットワークへの攻撃を行っているものとされている。これはサイバー攻撃がその後の武力攻撃等を見据えた前段階のものとして行われる可能性があることを示唆している。中国は、これまで軍事関連企業、先端技術保有企業等の情報窃取のためにサイバー攻撃等を行っているとみられ、2024 年には同国が支援する「SaltTyphoon」が、世界中の電気通信事業者、政府機関等の情報システム・ネットワークを標的としていることが明らかとなった。また、2023 年に同国を背景とすると指摘される「VoltTyphoon」が、Living Off The Land（システム内寄生戦術）[9]を用いてグアム等の米軍・政府機関や重要インフラ事業者に長期間侵入したとされる事例に見られるように、同国は有事に備え重要インフラ等の機能妨害・機能破壊も視野に入れた攻撃キャンペーンを行っているという評価も出てきている。さらに、北朝鮮は、暗号資産の窃取や、外国に派遣した IT 労働者が身分を偽って仕事を受注すること等を通じて、不法な資金の調達を図っており、こうした収入が核・ミサイル開発に利用されているこ

批判：客観性を欠くサイバー攻撃の事実例示

本案ではロシア、中国などからの具体的なサイバー攻撃について言及がある。しかし、一般に、当事者が自ら名乗りをあげるケースは実空間での攻撃に比べて圧倒的に少なく、国際法上攻撃の責任を負うべき国家が認定されている場合は別にして、責任の帰属に争いがある**微妙なアトリビューションの問題について、本案のように、サイバー攻撃の敵として断定的に特定の国家を名指しすることの妥当性**には疑問が残る。

同時に、本案で例示されているサイバー攻撃は、具体的に言及された国々だけで実践されてきたものではなく、当然想定されるように、**同様の攻撃を米国をはじめとする西側諸国も行なっているはず**である。このことが公表されていないことこそが問題だというセキュリティの専門家の指摘もある。この点で、本案の記述は、**国際的に対立関係にあって双方が行なっているサイバー攻撃の現状を客観的に俯瞰して分析したものとはいえず**、現政権のイデロギーに強く影響されたものであり、本案の信頼性を損いかねない。

目的達成のための施策

1．深刻化するサイバー脅威に対する防御・抑止

(1)国が要となる防御・抑止

①インシデント対処の高度化による被害の拡大・深刻化の防止

- ✓ 新法に基づく基幹インフラ事業者等による国への特定重要電子計算機の届出やインシデント報告のための基盤整備。報告様式・報告先の一元化
- ✓ 脆弱性情報の集約・整理・分析。政府が率先して民間事業者等への被害防止に効果的な情報提供

②通信情報を含むサイバーセキュリティ関連情報の集約、効果的な分析と活用

- ✓ NCOに情報集約。分析能力を抜本的に向上させる体制の構築
- ✓ 通信情報の利用により、攻撃態様の把握等を目指し、アクセス・無害化措置にも有効な分析を実施
- ✓ 法令・必要性を踏まえ、政府部内、同盟国・同志国等、協定*当事者、新協議会構成員、電子計算機等供給者等に率先して分析結果を提供

*新法に基づき基幹インフラ事業者等から通信情報の提供を受けるための協定

③アクセス・無害化措置を始めとする多様な手段を組み合わせた能動的な防御・抑止

- ✓ アクセス・無害化措置について、我が国の総力を十全に活用すべく、能力を有する警察と防衛省・自衛隊が共同で実施する体制を構築。国家安全保障との整合性を確保し、サイバー安全保障担当大臣の下、NCOがNSSと連携し総合調整機能を発揮し、統一方針により国際法上許容される範囲内で実施。能力の大幅強化、システム・資機材等の速やかな整備
- ✓ NCOが総合調整機能を発揮し、従前からの施策（任意のﾃｲｸﾀﾞｳﾝ、ﾊﾟﾌﾞﾘｯｸ･ｱﾄﾘﾋﾞｭｰｼｮﾝ、攻撃手口の公表等）と適切に組み合わせ、関係府省庁や同盟国・同志国等と緊密に連携しつつ能動的な防御・抑止を実施
- ✓ 能動的な防御・抑止に必要な訓練・演習の実施、先端技術の活用検討

④体制・基盤・人材等の総合的な整備・運用

- ✓ サイバー安全保障の確保に持続的・的確に取り組むため、必要な体制・基盤・人材等の総合的整備
- ✓ サイバー通信情報監理委員会に対する平素からのサイバーセキュリティ情勢等の情報共有、認識共有

(2)官民連携エコシステムの形成及び横断的な対策の強化

①官民間の双方向・能動的な情報共有と対策強化のサイクルの確立

- ✓ 官民間の複層的対話の継続的な実施。緊急時に初めて連携を模索するのではなく、平素から信頼関係構築。新法に基づく協議会等を活用し、国から積極的な脅威情報等の提供とともに、官民間の情報共有基盤を整備

②官民における脅威ハンティングの実施拡大

- ✓ 脅威ハンティングの普及促進、実施等に関する基本方針を策定。能動的サイバー防御の手段としての位置づけの明確化、セキュリティ能力を向上

③演習の体系的な実施

- ✓ 分野を横断して効率的・効果的な演習実施を可能に。演習ノウハウや成果の相互共有を促進

(3) 国際連携の推進・強化

①同盟国・同志国等との情報・運用面での協力

- ✓ 我が国の対処能力向上に資する各国関係機関との継続的な対話、多国間会合等を通じた協力、国際共同捜査の推進、悪意あるサイバー活動の抑止に向けたパブリック・アトリビューションや外交的対応等の取組強化

②インド太平洋地域におけるサイバー安全保障分野の対応能力向上の支援・推進

- ✓ ASEANを含むインド太平洋地域の安定と繁栄が我が国の発展の基盤であることを踏まえ、AJCCBC*等を通じた能力構築支援を強化

*日ASEANサイバーセキュリティ能力構築センター

③国際的なルール形成の推進

- ✓ 我が国の基本的理念の発信とともに、サイバー空間に係る法の支配の推進、国際社会のルール形成における積極的な役割を果たす

サイバー安全保障担当大臣　松本　尚

NCO　国家サイバー統括室（次頁参照）

https://www.cyber.go.jp/index.html

NSS　国家安全保障局

https://www.cas.go.jp/jp/gaiyou/jimu/anzenhosyou.html

国家安全保障会議を恒常的にサポート。内閣官房の総合調整権限を用い、国家安全保障に関する外交・防衛・経済政策の基本方針・重要事項に関する企画立案・総合調整に専従。

NCO とは

NCO とは ※ NCO ： National Cybersecurity Office

「 近年、サイバー攻撃による政府や企業の内部システムからの情報窃取等が大きな問題となっているほか、重要インフラ等の機能を停止させることを目的とした高度な侵入・潜伏能力を備えたサイバー攻撃に対する懸念が急速に高まっています。特に、重要インフラの機能停止や破壊等を目的とした重大なサイバー攻撃は、国家を背景とした形でも日常的に行われるなど、安全保障上の大きな懸念となっています。

こうした情勢に対応するため、「国家安全保障戦略」（令和４年 12 月 16 日閣議決定）において、内閣サイバーセキュリティセンターを、サイバー安全保障分野の政策を一元的に総合調整する新たな組織に発展的に改組することとされたところ、2025（令和７）年５月のサイバー対処能力強化法等の成立も踏まえ、2025（令和７）年７月、内閣サイバーセキュリティセンターを改組し、内閣サイバー官を長とする「国家サイバー統括室」を設置しました。

NCO の主な所掌事務は、サイバーセキュリティ戦略本部の事務局としての役割のほか、行政各部の情報システムに対する不正な活動の監視・分析やサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助、監査等を行うとともに、サイバーセキュリティの確保に関する総合調整役を担っています。

https://www.cyber.go.jp/



批判：日本はサイバー攻撃を憲法上禁じられている

本案は、現状のいわゆる地政学的な脅威に対して、日本もまたサイバー領域におけるより一層の攻撃主体となることを宣言するものとなっている。**本案は、地政学的な脅威を高め、結果として国家や国家を後ろ盾とするサイバー攻撃のアクターの動機を刺激する**ことに帰着する。本案の掲げる戦略は、「自由、公正かつ安全なサイバー空間」や「５つの原則」（「法の支配」等）を守る」(p.4) という目的とは矛盾し、「自律性」「多様な主体の連携」原則にも反する。

戦争を放棄し、戦力を保持しないという憲法９条の規定は、サイバー領域の戦争にも適用されるべきものである。しかし、**日本政府は、一方で東アジア地域の緊張を刺激するような自衛隊の戦力拡大、外国の軍隊 (米軍) への領土の提供**と特権付与などの政策をとりつづけている。国家がなすべきなのは、サイバー領域を含む軍事的な緊張を、暴力の手段ではなく、外交など対話の手段によって解決する高度な政治的な取り組みである。

攻撃者が優位にある

戦略(案)の記述

アクセスが可能となり、我々に多くの利便をもたらしている。これまで以上にサイバー空間と実空間は密接に融合し、AI や量子技術等の先端技術が、デジタルサービスや産業に大きなインパクトを与えようとしている。

　その一方、このサイバー空間では、相対的に露見するリスクが低く攻撃者側が優位にあるサイバー攻撃の脅威も急速に拡大している。この脅威は、今日の複雑な国際情勢や、我が国が置かれている安全保障環境の文脈においても、大きな懸念となっている。

批判：攻撃者が優位とはいえない

政府はサイバー領域の軍事安全保障では繰り返し「攻撃者が優位」という主張を展開し、日本が攻撃者となる必要性を強調してきた。この発想は、そもそも専守防衛の主張と矛盾する。（この点を護憲派野党が的確に批判できていない）

本案で前提されている攻撃者が優位、という主張は間違いである。本案では、**実際には攻撃の圧倒的に多くは防御できていることに言及せず**に、防御できなかったケースについてのみ注目することによって、あたかも攻撃に日本が対処できていないかのような間違った印象を与えている。しかも、**なぜ攻撃を防げなかったのか、という肝心の原因についても説明をしていない**。実際には、防御に失敗した多くの事例では、セキュリティの現場で適切な対策を怠ったケースが多くみられ、**警察や自衛隊などや政府のセキュリティ関連組織が主導する必要もなく防御ができているはずの事例が多い**。この事実にほとんど言及せず、あたかも攻撃は最大の防御なり、という古い諺をサイバー領域に持ち込み、**民間や個人ではセキュリティの対処ができないかのような印象操作**となっており、サイバー領域のセキュリティリスクを高める結果になっている。

「脅威ハンティング」という名のサイバー攻撃

戦略(案)の記述

② 官民における脅威ハンティングの実施拡大

近年、我が国の官民組織を対象に「Living Off The Land 戦術」（システム内寄生戦術）のような高度なサイバー攻撃が行われ、経済社会、国民生活、ひいては国家安全保障に悪影響を及ぼす脅威アクター（以下「高度脅威アクター」という。）が観測されている。

既存のセキュリティ対策を適切に実施することが重要であることは言うまでもないが、このようなサイバー攻撃は既存のセキュリティ対策を回避するものが少なくない。こうした中、検知を回避し侵入・潜伏した攻撃痕跡等を探索することによってサイバー攻撃の被害を検知する手法であり、かつ、アクセス・無害化措置を始めとする能動的サイバー防御に資する情報を得る手段として有効である「脅威ハンティング」を実施していく必要がある。特に、高度脅威アクターの標的となる政府機関、独立行政法人、サイバー安全保障を確保する上で重要な民間事業者等における脅威ハンティングの必要性は高いと認められる。そのため、脅威ハンティングの普及促進、実施等に関する基本方針を 2026 年夏を目処に策定する。

脅威ハンティングについては下記を参照

「脅威ハンティング実践のすゝめ」独立行政法人情報処理推進機構 産業サイバーセキュリティセンター、https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2025/j5u9nn00000052sf-att/j5u9nn000000531o.pdf

批判：日本も攻撃者になることのリスク

本案は、サイバー攻撃では「相対的に露見するリスクが低く攻撃者側が優位」にあるとの基本的な立場をとる。このことから、上記の攻撃の例示は、**日本もまた同様の攻撃者となることを通じて、優位にたつことを意図している**ことと解せる。この場合、**日本も露見のリスクを回避する攻撃、いわゆるアクセス・無害化などのサイバー攻撃を実施する**ことで優位な攻撃者の立場を確保することになるはずである。

また高度なサイバー攻撃の例として**Living Off The Land などを例示し、日本のサイバー攻撃においてもこうした高度な攻撃手法を用いることが予想できる。こうした攻撃には長期にわたり標的のネットワークに潜伏してデータを窃取するなどのスパイ活動も含まれる。こうした手法を用いるかどうか**について、本案は、用いるとも用いないとも明言していないが「**脅威ハンティング**」は事実上こうした行為も含意可能だ。**相手が用いる攻撃手段に対して、それと同等かそれ以上の能力をもつ手段によって対処する**ことが軍事的な優位を確保することになるという本案の考え方からすれば、このようなサイバー攻撃の可能性は否定できない。本案は日本の攻撃手法について一切沈黙しているが、これは重要な争点になりうる問題であり、明らかにすべきだ。

批判：日本のサイバー攻撃はサイバー攻撃の応酬という泥沼を招く

本案では、日本がサイバー攻撃（アクセス・無害化を含む能動的サイバー防御と呼ばれる事態）を可能とする体制の構築によって、相手国からのサイバー攻撃を今以上に撃退できると述べている。しかし、実際には逆効果にしかならない。**日本のサイバー攻撃は相手による反撃の動機を刺激し、攻撃の応酬から実空間における軍事的な緊張へと、戦争を誘引するきっかけになりかねない。**しかもこの攻撃・反撃の過程は、実空間での武力衝突とは異なり、数ヶ月から数年の単位で、長期にわたって水面下で、身元も秘匿して遂行される。つまり、日本のサイバー攻撃もまたこうした手法をとるはずである。結果的に、こうしたサイバー攻撃は、よりいっそう深刻なサイバー領域のリスクを長期にわたって高めることにしか繋がらない。しかも、**こうした攻撃・反撃のサイバー領域の「戦場」には国境がなく、日本の国内と国外にまたがって起こされることになる。日本のサイバー攻撃では通信情報の利用が前提条件とされているから、こうしたリスクの高まりは、通信の秘密を侵害する通信情報の政府によるより一層の利用に繋がり、政府によるコミュニケーションへの監視の強化を招き、自由な通信環境も民主主義の基盤となる言論・表現の自由もより脆弱なものに**なる。

目的達成のための施策

2．幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

(1)政府機関等におけるサイバーセキュリティ対策の強化

①対策水準の向上と継続的な見直し

✓ 政府統一基準群等の継続的な見直し。監視の結果等を活用したメリハリのある監査。外局や地方支分部局等を含めた措置の徹底・改善。
機密性の高い情報の取扱いの検討

②政府機関等の監視体制・インシデント対応力の更なる強化・高度化

✓ CYXROSSセンサーの導入による監視・分析等、GSOCによる政府横断的な不正な通信の監視等の取組の強化・高度化

③強靭な政府情報システムの構築と運用

✓ デジタル庁は監視・脆弱性管理等により重要なシステムのセキュリティ等強化。各政府機関は適切な水準が確保されたシステムを構築・運用

④政府機関等におけるサイバーセキュリティ人材の育成・確保と体制の強化

✓ サイバーセキュリティ人材の定義を明確化したうえで、研修や演習の充実・強化・人材の官民交流等に活用

(2) 重要インフラ事業者・地方公共団体等におけるサイバーセキュリティ対策の強化

①重要インフラ事業者等におけるサイバーセキュリティ対策の強化

✓ 重要インフラ統一基準の新規策定。PDCAサイクル構築による、重要インフラ分野全体のセキュリティ水準引上げ

②地方公共団体におけるサイバーセキュリティ対策の強化

✓ 自治体情報セキュリティクラウドの円滑な更新に向けた財政的な支援。デジタル人材の確保・育成に対する支援。脆弱性等診断システム構築

③大学等におけるサイバーセキュリティ対策の強化

✓ サイバーセキュリティ対策や体制整備等に関する助言・情報共有。研修・訓練の実施。事案発生時の助言等の支援

(3)ベンダー、中小企業等を含めたサプライチェーン全体のサイバーセキュリティ及びレジリエンスの確保

①セキュアバイデザイン原則等に基づくベンダー等における責任あるサイバーセキュリティ対策の取組の推進

✓ 情報システム等供給者の責務浸透に向けた制度構築。
「JC-STAR」制度の更なる制度構築と社会全体での活用促進。
SBOMの活用や安全なソフトウェア開発の促進

②サプライチェーンを通じたサイバーセキュリティ及びレジリエンスの確保

✓ サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度の整備、普及促進。
取引先企業への対策要請等に係る関係法令の適用関係の明確化

③中小企業を始めとした個々の民間企業等における対策の強化

✓ ガイドライン等の整備・ひな形の提示。
サイバーセキュリティお助け隊サービスの利用改善に向けた見直し。

(4)全員参加によるサイバーセキュリティの向上

✓ 産学官民の多様な主体による積極的な連携・協働、普及啓発・情報発信
✓ 環境変化や多様なニーズに合わせて各コンテンツを適切にアップデート
✓ 情報セキュリティを含む情報教育の充実

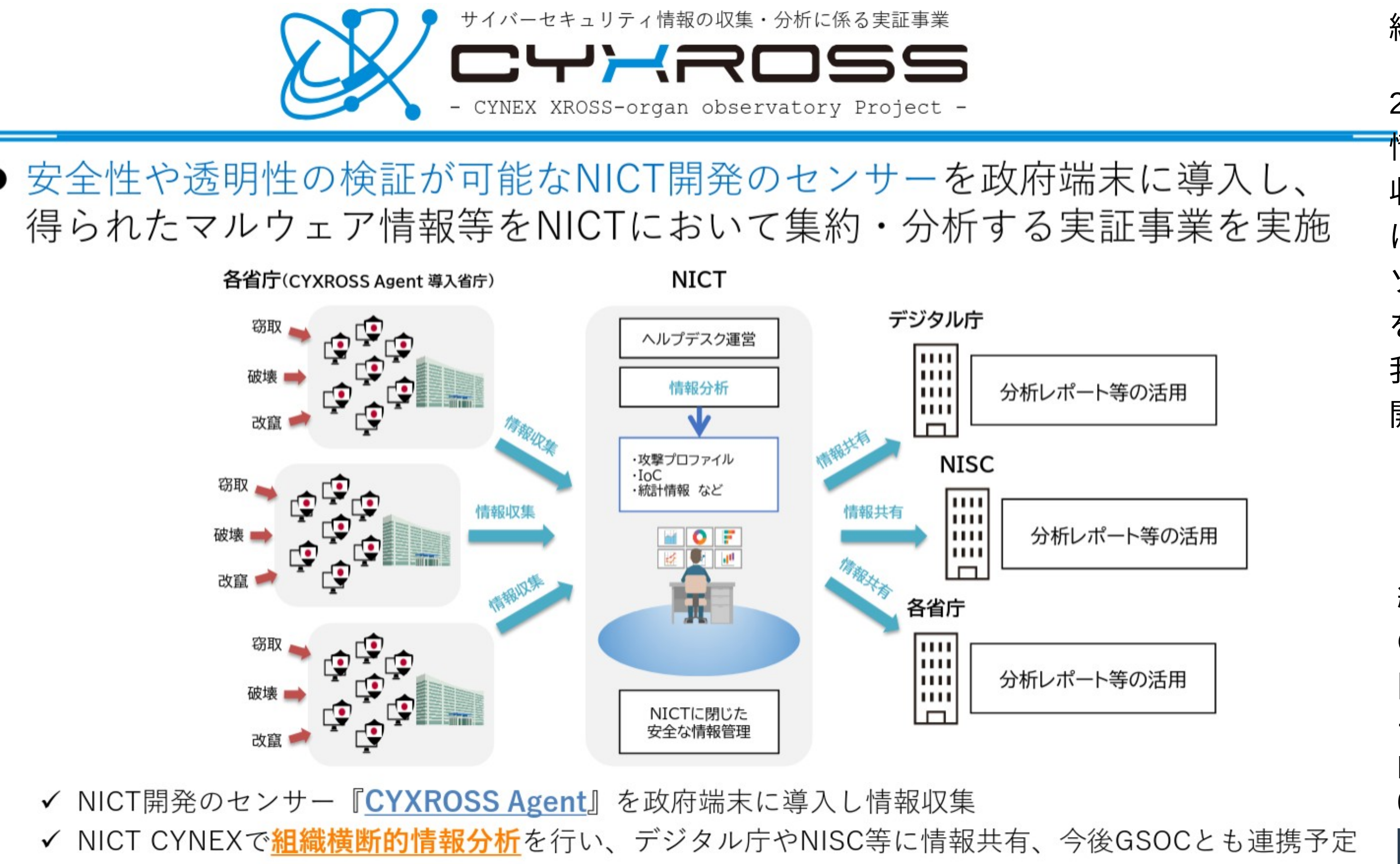
(5)サイバー犯罪への対策を通じたサイバー空間の安全・安心の確保

✓ 匿名性を悪用する犯罪者グループ、犯罪インフラを提供する悪質事業者等に対する摘発を始め、サイバー犯罪へ適切に対処するとともに、捜査能力・技術力の向上に取り組む

JC-STAR:セキュリティ要件適合評価及びラベリング制度。インターネットとの通信が行える幅広いIoT製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的(IPA https://www.ipa.go.jp/security/jc-star/index.html)

SBOM:Software Bill of Materials ソフトウェア部品表(経産省)https://www.meti.go.jp/policy/netsecurity/wg1/SBOMv2.pdf

CYXROSS とは何なのか？

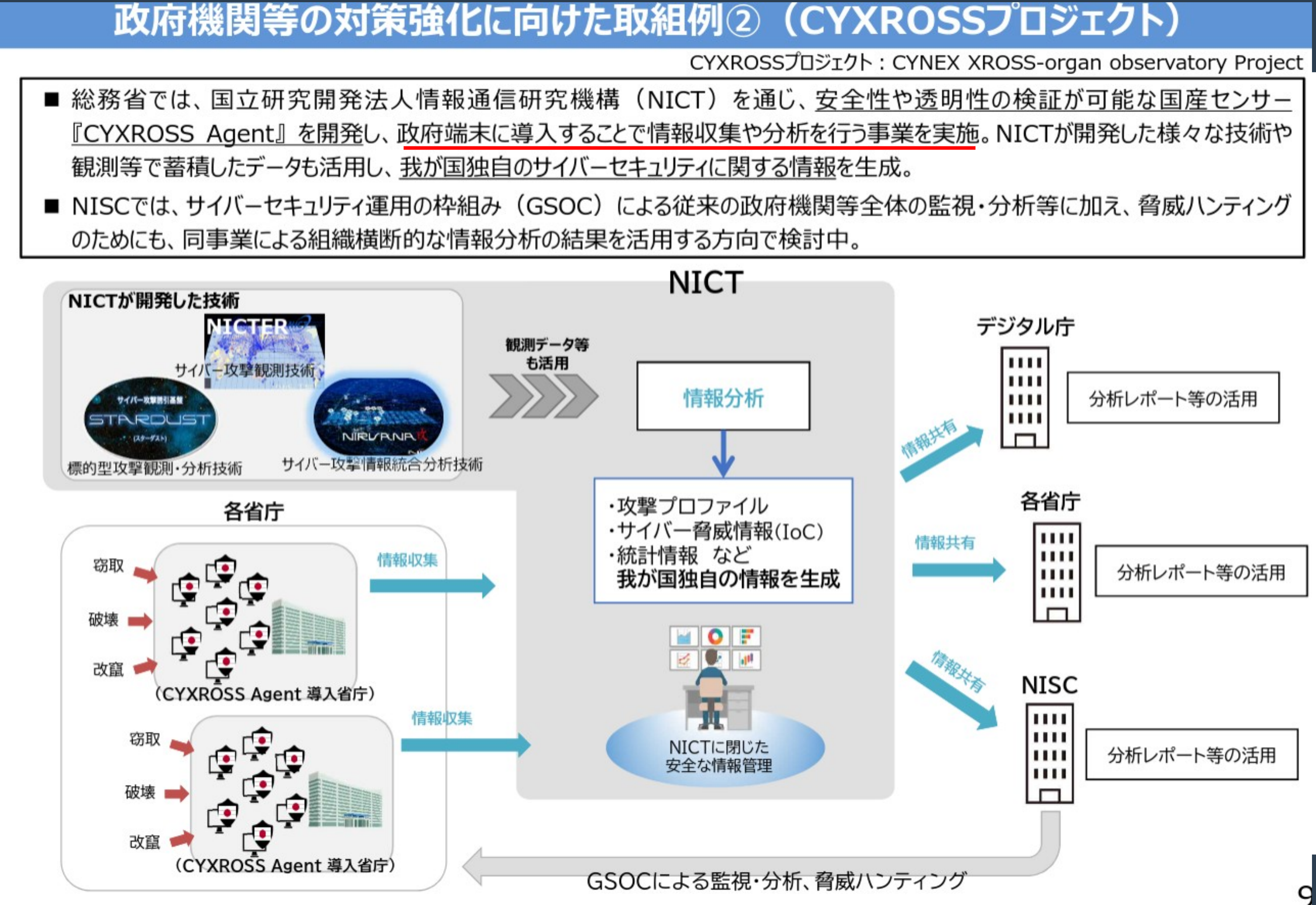


総務省情報通信白書 2023 年

2023 年度（令和 5 年度）より、「政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業 (CYXROSS) 」について、一部の府省庁に国産セキュリティソフトを導入し、得られたマルウェア情報等を NICT の CYNEX へ集約・分析することで、我が国のセキュリティ対策を強化する取組を開始

「NICT サイバーセキュリティ研究所の取り組み - CYNEX, CYXROSS, AI x Cybersecurity -」
国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所長 井上 大介
https://www.soumu.go.jp/main_content/000952545.pdf

CYXROSS とは何なのか？



CYXROSSはサイバー領域における標的システムへの「武器」に転用可能かどうかを注視したい

GSOC: 政府関係機関情報セキュリティ横断監視・即応調整チーム。各機関に設置したセンサーを通じた政府横断的な監視、攻撃等の分析・解析、各機関への助言、各機関の相互連携促進及び情報共有を行う

サイバー安全保障分野での対応能力の向上に向けた有識者会議 官民連携に関するテーマ別会合 第2回参考資料 2024年７月23日
内閣官房サイバー安全保障体制整備準備室
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai3/siryou4-3.pdf

批判：実害の回避に必要なのは適切なセキュリティ管理だけで十分

攻撃が実害となってしまうケースの多くは、**適切なセキュリティの設定・管理がなされていなかった**などによるものである。パスワードを適切に設定する、セキュリティのアップデートを行う、サポート終了の機器やソフトウェアを使わないなど基本を遵守することで実害を回避できるケースが多い。これらは、**私たち市民一人ひとりの場合も、企業や団体の場合も、対処可能な対策であり、政府が国家安全保障や、ましてや軍事的な政策の一環として軽々に位置付けるべきものではない。**

（参考・右図）アサヒグループへのランサムウェア攻撃事例を

記者会見から考察～今、注意すべき「データセンター」への侵害

https://www.trendmicro.com/ja_jp/jp-security/25/l/expertview-20251218-

項目	内容
発生日時	2025年9月29日午前7時頃。
発見経緯	発生したシステム障害に対する調査で暗号化ファイルを確認。
初動対応	9月29日午前11時にネットワーク遮断、データセンター隔離措置。
侵入経路	システム障害発生の約10日前に、グループ内の拠点にあるネットワーク機器を経由（通過）し、アサヒグループのネットワークに侵入したことが判明。 その後、アサヒグループの**主要なデータセンター**に侵入した。
内部活動	パスワードの脆弱性を悪用し、管理者権限を奪取した。 奪取した管理者アカウントを不正利用してネットワーク内を探索し、主に業務時間外に複数のサーバへの侵入と偵察を繰り返した。
情報窃取	データセンターを通じて従業員に貸与している一部のPC（パソコン端末）のデータが流出した。 データセンターにあるサーバ内に保管されていた個人情報については、流出の可能性があるものの、現時点でインターネット上に公開されたといった事実は確認されていない。
ランサムウェア実行	侵入されたアクセス権を認証するサーバからランサムウェアが一斉に実行された。 起動中の複数のサーバやPCの一部のデータが暗号化された（PCの台数は37台）。

アサヒグループへの攻撃でも、機器の脆弱性やパスワード管理の不備を衝かれた可能性が高い

批判：セキュアバイデザイン原則によりプライバシーバイデザインが後回しに

一般に、国家安全保障を重視する政策と技術の導入は、個人のプライバシーや通信の秘密の権利を損うものとなることが知られている。本案はもっぱら**国家安全保障のみを重視する「セキュアバイデザイン」の立場をとっている**ために、**通信の秘密やプライバシー・個人情報の権利が犠牲**にされており、ほとんど実質的な言及も関心ももたれていない。

通信技術などについても、**通信情報の収集やサイバー攻撃を可能にするといった意味での国家安全保障を優先**した技術仕様を優先させており、その結果としてプライバシーを重視した仕様がないがしろにされ、人々のコミュニケーションの権利が脆弱となる危険性がある。

しかも**セキュアバイデザインの基本的な目的は、日本がサイバー攻撃の主体となるために必要な制度構築**でしかない。結果として、前述したように、日本によるサイバー攻撃が、相手国による反撃を招き、この攻撃・反撃の応酬にサイバー領域が巻き込まれ、**プライバシーバイデザインが更に疎かに**され、結果として、世界中の市民ひとりひとり、とりわけ社会のなかで人権が制約されている社会的マイノリティのサイバーセキュリティ（**サイバー・ピープルズ・セキュリティ**）がより一層のリスクを被る結果になりかねない。

批判：人々のサイバーセキュリティを脆弱にする国家のサイバーセキュリティ戦略は容認できない

本案全体として、**サイバー領域におけるコミュニケーションの主体でもある個人の権利への関心が全くない。**もっぱら関心は、国家にとってのサイバーセキュリティでしかない。すでによく知られているように**国家安全保障（ナショナル・セキュリティ）は、人々の安全保障（ピープルズ・セキュリティ）とは異なる観点と相反する利害を有し**、対立することもある。サイバー領域においても同様であり、国家安全保障の観点から日本政府がサイバー攻撃を導入しようとする方向をとることに対して、サイバー領域における人々の安全保障（ピープルズ・セキュリティ）は、**平和なコミュニケーション領域を確保し、普遍的な人権として確立している自由や平等の権利を保障し、差別や憎悪を排除すること**である。しかし、本案は、むしろ日本のサイバー攻撃を合法化・制度化する結果として、地域の緊張を高め、サイバーと実空間における軍事的な敵対関係を煽るものになりかねない。また、サイバー攻撃を含むハイブリッドな戦争において、日本国内の差別や偏見、憎悪を煽るような言動や相手国に対する偽情報を含む「情報戦」に日本政府が事実上加担し、サイバー領域における深刻な人権侵害を加速化することを正当化するものになりかねない。結果として、国籍や民族などに関わらずに、人々が相互に自由に繋るためのサイバー領域のコミュニケーションの権利そのものが深刻な侵害を被ることになる。

以上、本案は、憲法９条に反して日本のサイバー攻撃をもっぱら加速化させ、人々のサイバー・セキュリティをより一層脆弱にするものと言わざるをえず、本案全体に対して反対である。

政府と企業に依存するサイバーセキュリティからの離脱が必要

政府
政府機関
国益優先

統制：法と官僚組織

民間企業
企業利益優先

個人
普遍的な人権
生存権
通信の秘密、言論表現の自由、思想信条の自由など

国境を越えた領域
実空間/サイバー空間

国家サイバーセキュリティ
Vs
民衆のサイバーセキュリティ